A Report
to the
Montana
Legislature

Information Systems Audit

Lottery Security

Montana State Lottery
Department of Administration

September 2018

Legislative Audit
Division

18DP-02

Information Systems Audits

Information Systems (IS) audits conducted by the Legislative Audit Division are designed to assess controls in an IS environment. IS controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. We conducted this IS audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our finding and conclusions based on our audit objectives. Members of the IS audit staff hold degrees in disciplines appropriate to the audit process.

IS audits are performed as stand-alone audits of IS controls or in conjunction with financial-compliance and/or performance audits conducted by the office. These audits are done under the oversight of the Legislative Audit Committee, which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of six members of the Senate and six members of the House of Representatives.

Audit Staff

Miki Cestnik
Diedra Murray
T. Shane Somerville

Reports can be found in electronic format at:
http://leg.mt.gov/audit

LEGISLATIVE AUDIT DIVISION

Angus Maciver, Legislative Auditor
Deborah F. Butler, Legal Counsel

Deputy Legislative Auditors
Cindy Jorgenson
Joe Murray

September 2018

The Legislative Audit Committee
of the Montana State Legislature:

We conducted an information systems audit of Montana State Lottery security operations. Montana law requires the Legislative Audit Division to perform a comprehensive security audit of the Montana Lottery every two years. We reviewed security controls within the 18 security areas defined by statute, including Lottery's computer systems, scratch and online tickets, and Lottery personnel and sales agents.

This report contains eight recommendations for strengthening information system and physical security at Lottery headquarters. These include improving processes to better identify potential risks to Lottery information systems, defining employee information system security responsibilities, and reducing risks related to unauthorized access to information systems and Lottery headquarters. A written response from the Montana Lottery is included at the end of the report.

We wish to express our appreciation to the Montana State Lottery personnel for their cooperation and assistance during the audit.

Respectfully submitted,

/s/ Angus Maciver

Angus Maciver
Legislative Auditor

Room 160 • State Capitol Building • PO Box 201705 • Helena, MT • 59620-1705
Phone (406) 444-3122 • FAX (406) 444-9784 • E-Mail lad@mt.gov

Table of Contents

Figures and Tables

Figures

Tables

Appointed and Administrative Officials

Montana State Lottery	Angela Wong, Director	
	Bryan Costigan, Security Director	
	Phil Charpentier, Information Technology Director	
Department of Administration	John Lewis, Director	

			Term Expires
Lottery Commission	Wilbur Rehmann, Chair	Helena	January 1, 2021
	Thomas Keegan, Attorney at Law	Helena	January 1, 2022
	Leo Prigge, CPA	Butte	January 1, 2019
	Jessika Kynett, Law Enforcement	Livingston	January 1, 2021
	Jean Price, Public Representative	Great Falls	January 1, 2022

Montana Legislative Audit Division

Information Systems Audit

Lottery Security

Montana State Lottery
Department of Administration

September 2018 18DP-02 Report Summary

In recent years, the Montana State Lottery has integrated more technology in to Lottery game management and player interaction. However, information security management has not developed at the same speed. As a result, significant improvements in Information Technology (IT) risk assessments and security policies and procedures are needed, including access management procedures, to ensure the Lottery strengthens operational integrity, and continues to generate revenue for the state of Montana.

Context

The Montana State Lottery (Lottery) was created in 1987. The Lottery transferred $12.3 million in fiscal year 2016 and $9.2 million in fiscal year 2017 to the general fund. The Lottery offers several types of games with different ways to play including scratch tickets, self-serve terminals, and instant game terminals. The Lottery manages these games with a central gaming system and an independent back-up system for verification of the central gaming system. This requires computer servers that need to be secured at multiple locations, various systems to manage security and gaming operations, and separation of tasks, system access, and physical hardware.

Montana law requires the Legislative Audit Division perform a comprehensive security audit of the Lottery every two years. We assessed risks related to the 18 defined areas within statute and found issues relating to internal control procedures and how users are managed for the various systems the Lottery operates. Our testing included comparing current procedures to state policy requirements and reviewing internal procedures that identify information security risks.

Results

The Lottery has established separate organizational divisions responsible for security and information technology (IT), but has not clearly established how IT security responsibilities are divided between the two. As a result, physical security procedures are generally well-developed, but information security practices need to be improved in several areas, including:

- Assigning information security responsibilities for different staff positions,
- Developing an IT risk assessment process,
- Formalizing IT security policies and procedures, and
- Enhancing access management and user accountability procedures, including those tied to contractors.

Recommendation Concurrence	
Concur	8
Partially Concur	0
Do Not Concur	0

Source: Agency audit response included in final report.

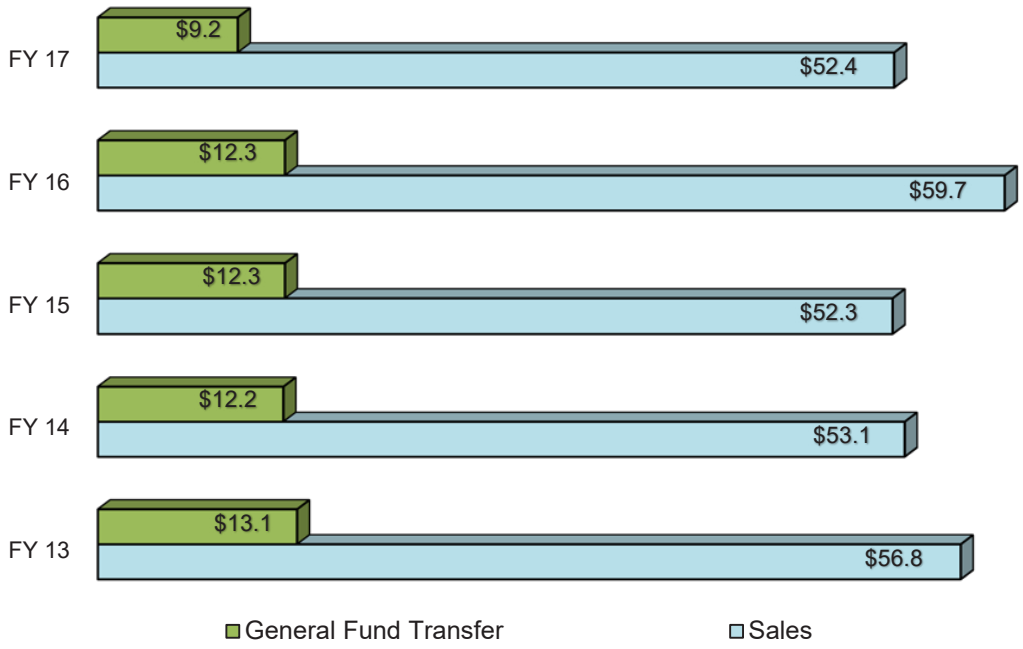
For a complete copy of the report (18DP-02) or for further information, contact the Legislative Audit Division at 406-444-3122; e-mail to **lad@mt.gov**; or check the web site at **http://leg.mt.gov/audit**
Report Fraud, Waste, and Abuse to the Legislative Auditor's FRAUD HOTLINE
Call toll-free 1-800-222-4446, or e-mail **lad@mt.gov.**

Chapter I – Introduction and Background

Introduction

The Montana State Lottery (Lottery) was created in 1987 and generates revenue through the sale of various types of lottery tickets. Its net revenues are transferred to the state's general fund and it has also contributed significant funds to various state programs. In fiscal year 2017, the Lottery transferred $9.2 million to general fund and $12.3 million in 2016. Lottery sales and general fund transfers for the last five years are shown in the figure below.

Figure 1
Lottery Sales Revenues and General Fund Transfers (in millions)
Fiscal year 2013 through 2017



Source: Compiled by the Legislative Audit Division.

Sales for fiscal year 2016 spiked due to a $1.5 billion jackpot and have since dropped back to a more average number.

Background

The Lottery is allocated to the Department of Administration and Lottery's director is appointed by the governor. The governor also appoints a five-member commission to oversee Lottery operations, set policy, and authorize games. The director administers the five divisions of the Lottery: Sales and Marketing, Administration, Finance, Security, and Information Technology (IT).

The Security Division includes a director of security and a criminal investigator position that address security within various areas of Lottery: building and warehouse security, game operations and general Lottery procedures, personnel, and computer systems. The IT Division consists of three staff that support all Lottery functions by working closely with the contractors to oversee game operations, test functionality, and assist with daily IT needs of the agency.

There are over 900 retailers in the state of Montana that offer opportunities to play Lottery games as well as a website with a player's club that includes promotional games and second chance drawings. Lottery offers several games that can be played in various ways through scratch tickets, self-serve terminals, and instant game terminals.

Lottery games currently include:

Lotto Games: Numbers are picked from a range of numbers and payouts depend on the number of players in the game and number of matches a player picks. Montana offers state level lotto games, such as Montana Millionaire and Big Sky Bonus, and multi-state games, like Powerball and Mega Millions. The Lottery is part of the Multi-State Lottery Association (MUSL) to help provide these types of games. This allows for bigger payouts and consistent administration of Lottery operations.

Instant Scratch Tickets: These are offered at licensed retailers through purchasing the physical ticket at the counter or through a self-service game terminal. Scratch ticket games are produced by a lottery gaming contractor, while self-service game terminals are provided and maintained by the central gaming system contractor.

Instant Win Games: These were previously referred to as "EZ Play," but are now called Treasure Play games. These predetermined games provide instant results like a scratch ticket and are offered at taverns and casinos throughout the state. These games are played on a terminal and there are currently 344 of these terminals throughout Montana.

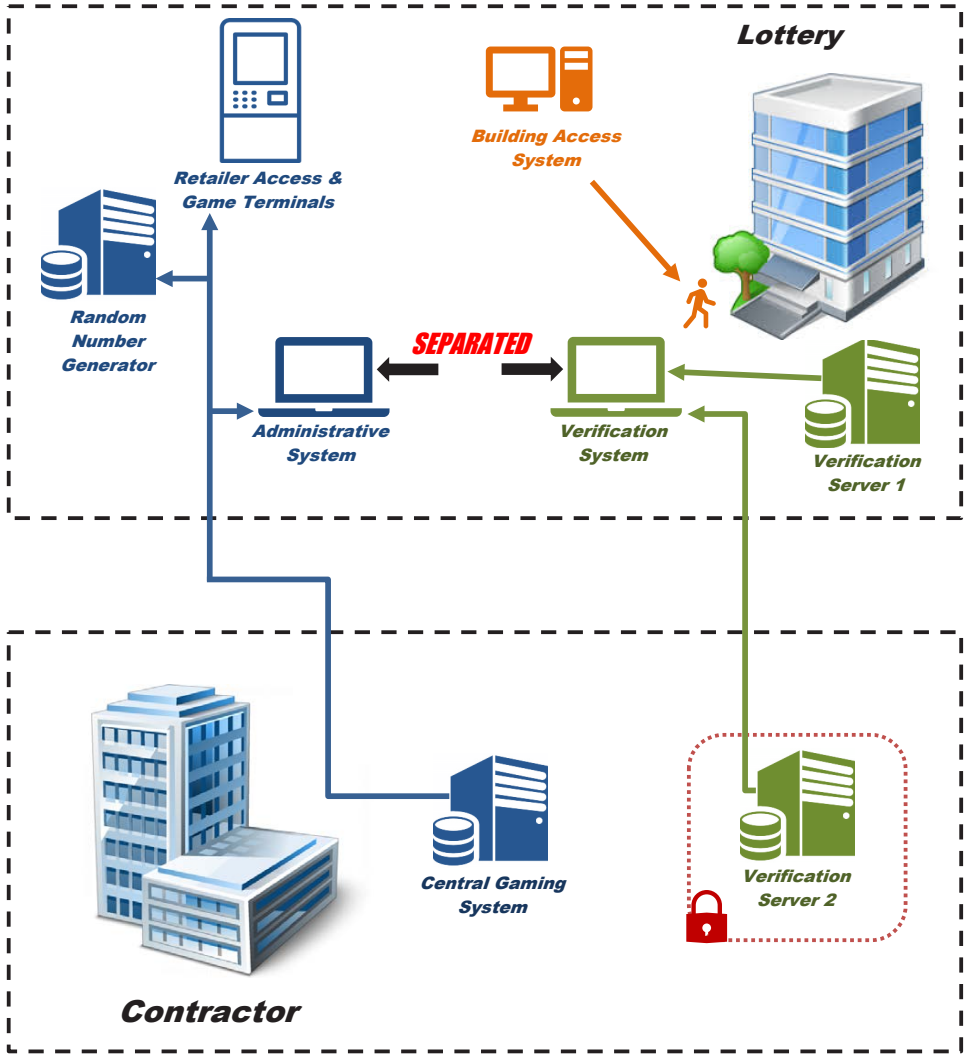
MUSL manages most of the lotto-style games that Montana Lottery provides and has established requirements that all states must meet and rules for state lottery operations to follow. MUSL also audits the states within the association. Every other year, MUSL auditors conduct an audit. Additionally, they require self-assessments from Lottery operations in the off years. Montana Lottery submitted a self-assessment in 2017 and hosted MUSL auditors for an on-site audit in January of 2018.

MUSL also requires gaming operations to be managed by a central gaming system with an independent back-up system for verification. This requires servers that need to

be secured at multiple locations, various systems to manage security as well as gaming operations, and separation of tasks, system access, and physical hardware.

The Lottery has a contract with a lottery vendor to provide this gaming system and all terminals and equipment used to administer games. The Internal Control System (ICS), used to verify and audit the central gaming system's processing, is subcontracted with a separate organization to maintain separation of the two systems. These two systems, along with others, are used to manage Lottery operations. The following figure shows the layout of these systems and their locations. The separation of ICS and the central gaming system is described below the diagram along with the operations of other systems.

Figure 2
Lottery Information Technology Operation Diagram



Source: Compiled by the Legislative Audit Division.

Central Gaming System (CGS): This is the system that manages all online games including game settings, data processing, reporting, and telecommunications with retailers. According to Lottery, CGS, and other Lottery systems, are closed systems that do not interact with outside systems or the internet.

Internal Control System (ICS): ICS independently processes the same data as CGS to verify results including online draws, balancing sales, and winners. ICS has three servers: one main server at Lottery and two servers housed with the CGS contractor for back-up and testing. The diagram shows these servers in the red box within the contractor area because, while they are housed there, the CGS contractor is not allowed to access them.

Back Office System (BOS): BOS is the administrative part of CGS and is used for administrative tasks like reporting, inventory tracking, and managing retailers and gaming terminals.

Badge Access System: This system maintains physical security at all doorways within the Lottery building in Helena through a multi-factor authentication system with both a physical key card and code.

Random Number Generators (RNGs): These servers contain code that generates random numbers for the Montana Lottery's lotto games (Montana Millionaire, Big Sky Bonus, and Montana Cash games).

Audit Scope and Objectives

The Legislative Audit Division is required to review the following 18 areas as part of a security audit every two years by §23-7-411, MCA:

1. Personnel security
2. Sales agent security
3. Contractor security
4. Security of manufacturing operations of contractors
5. Security against ticket or chance counterfeiting and alteration, and other means of fraudulently winning
6. Security of drawings among entries or finalists
7. Computer security
8. Data communications security
9. Database security
10. Systems security

11. Premises and warehouse security
12. Security in distribution
13. Security involving validation and payment procedures
14. Security involving unclaimed prizes
15. Security aspects applicable to each particular game
16. Security of drawings in games whenever winners are determined by drawings
17. The completeness of security against locating winners in games with preprinted winners by persons involved in their production, storage, distribution, administration, or sales
18. Any other aspects of security applicable to any particular Montana Lottery game and to the Montana Lottery and its operations

These areas were assessed for risks and existing safeguards including forms of risk in both physical and system security. Our assessment included defining multiple risks specific to Lottery in each area, identifying what controls currently exist, and determining the level of impact and likelihood the risk has with the related controls established by Lottery. Table 1 (see page 6) includes the summary of assessment work for each review area within statute at the time of planning the audit.

Each area is assigned a rating of:

- High–Significant potential risk
- Med–Moderate potential risk
- Low–Minimal potential risk

Table 1

Audit Risk Assessment Results for the 2018 Lottery Security Audit

Required Statute Areas	Risk Rating
Personnel security	Med
Lottery sales agent security	High
Lottery contractor security	Med
Security of manufacturing operations of lottery contractors	Low
Security against ticket or chance counterfeiting and alteration and other means of fraudulently winning	Low
Security of drawings among entries or finalists	High
Computer security	High
Data communications security	Low
Database security	High
Systems security	High
Lottery premises and warehouse security	High
Security in distribution	High
Security involving validation and payment procedures	Med
Security involving unclaimed prizes	Low
Security aspects applicable to each particular lottery game	Low
Security of drawings in games whenever winners are determined by drawings	Low
The completeness of security against locating winners in lottery games with preprinted winners by persons involved in their production, storage, distribution, administration, or sales	Med
Any other aspects of security applicable to any particular lottery game and to the lottery and its operations	High

Source: Compiled by the Legislative Audit Division.

The last area required by statute requires other aspects of security; therefore, we included general IT assessment work as it relates to Lottery and its operations. This assessment was conducted in the same manner as the risks specific to Lottery. The summary of this assessment work is shown below.

Table 2
General IT Assessment Areas for 2018 Lottery Security Audit

Assessment Area	Description	Risk Rating
Regulatory Requirements	Represents the amount of legal or contractual requirements of the system or data within the system as well as the level of complexity and volatility of those requirements and the impact on the ability to comply.	Med
Topic of Interest	Represents any interest from the legislature, the public, or other audit work.	Low
Security Management	Represents the level of risk associated with the security management and risk assessment procedures of an organization, as it relates to the specific system.	High
Impact of System Failure	Indicates the level of risk associated with errors in the system due to flawed, manipulated, or missing data; change control processes; and continuity of operations if affected by a disaster or system failure.	Med
Management/ Governance	Defined by the structure, oversight, and management procedures an agency has related to the topic/system.	Med
Fraud/Abuse	Shows the potential for fraudulent activity to occur based on review of fraud controls, likelihood of fraud or abuse due to the nature of the data or operations associated with the system, and historic information about the system or program.	High
Nature and Profile	Defined by the complexity, age, and cost of a system; number of users and levels of security within a system; criticality of system operations; sensitivity of the information processed; and the reliance on decisions a system executes.	Med

Source: Compiled by the Legislative Audit Division.

Reoccurring risks associated with access management (both physical and computer/logical) and risk management were rated high through this assessment. Based on the high-risk areas identified through assessment, the following objectives were developed:

1. Determine if internal control procedures are providing effective risk management and ensuring staff turnover does not impact the security of Lottery operations.
2. Determine if Lottery is ensuring physical and logical security through access management procedures related to applications, databases, and systems that manage physical building security.

Audit Methodologies

Methodologies for this audit included:

Interviews: Lottery staff and management from all divisions were interviewed to review procedures for security, risk management, and general Lottery operations.

Tours/Observations: Various procedures, including scratch ticket shipments and winner verification, were observed to ensure procedures were conducted securely. The Lottery building was recently remodeled in 2017, so the tour included reviewing changes made during the remodel. A tour of the contractor facility in Helena was conducted as well.

Requirements Review: We reviewed current Lottery processes for risk and access management to determine whether they meet requirements of applicable statutes, rules, and policies and procedures.

Comparison to Industry Standards: We compared various processes to industry standards to identify where they could be strengthened to better ensure the integrity of Lottery security. Industry standards used include:

- National Institute of Standards and Technology (NIST): Provides a catalog of security and privacy controls for information systems. Montana state policy requires the use of NIST as guidance for security risk management and has established baseline security controls from NIST.
- Control Objectives for Information and Related Technology (COBIT): Standards for Information Technology (IT) management and governance. These standards outline control practices to reduce technical issues and business risks.

Overall Conclusion

We determined the Lottery should make improvements to ensure changes do not impact security operations, and that access to Lottery systems and IT hardware is managed effectively. While Lottery has an IT director and security director, the responsibilities for Information Security are undefined and some are not being performed effectively. Assignment of key responsibilities and more emphasis and prioritization of IT security in the form of a risk assessment and required IT security policies and procedures are needed. To strengthen physical and logical security at the Lottery, staff will need to make improvements to access management procedures related to applications, databases, and systems that manage physical building security.

Report Contents

This report addresses findings in the following chapters:

- Chapter II – Lottery Risk Assessment Process
- Chapter III – Information Security Policies and Staff Responsibilities
- Chapter IV – Computer and System Access Management
- Chapter V – Physical Information Security Management

Chapter II – Lottery Risk Assessment Process

Introduction

When looking at information technology (IT) security risks, it is important to understand how different types of risks are identified, reviewed, and mitigated. This can include the specific technical elements of IT security, but also 'human' factors that affect all types of operations, such as staff turnover. To address our first objective, we reviewed the Montana State Lottery's (Lottery) internal processes to understand how its risk assessment process works, how the Lottery implements recommendations for improvements in managing risk, and how 'human' factors like staff turnover are addressed.

Lottery manages organizational risks through an internal control process. The supporting policy and procedures detail the history of the Lottery, in addition to spelling out the purpose and goals of the organization. Within the Lottery's internal control policy, there are five sub-sections describing the "Internal Control at the Entity Level" that include: 1) Control Environment, 2) Risk Assessment, 3) Control Activities, 4) Information and Communication, and 5) Monitoring. These sub-sections are designed to cover all risks that have an overarching or pervasive effect on the Lottery. Therefore, we used this document during fieldwork as the basis for understanding Lottery's IT risk management process.

Overall, we identified minimal formal risk identification for IT. We also found prior audit recommendations related to IT security and risks were not effectively implemented. Due to the recurring nature of the Lottery Security audit, prior audit recommendations are reviewed during the planning phase of each audit to determine implementation. While planning this audit, we identified the prior audit recommendations were partially implemented. Lottery staff indicated that security staff turnover impacted the implementation of these recommendations. However, we identified other contributing factors and the need for a more structured IT risk management process that also addresses recommendations given to Lottery. These are discussed in the following sections.

Risk Assessments Are Crucial to Maintain Lottery Security

The risk assessment section of the Lottery's internal control policy states an internal audit plan should be developed based on:

- Risk assessments of critical systems
- Reviews of internal, financial, and administrative systems and procedures

- Executive staff's assessment of existing risks
- Past internal audit experience

Industry standards for IT risk assessments adopted in state policy also include similar standards with more specific requirements related to IT, such as assessment of unauthorized use or modification of each information system. Having a properly instituted risk assessment process is important for the integrity of an organization. Risk assessment also helps smaller agencies, like Lottery, to prioritize and address the most business-critical risks and help to decide what risks to focus on.

Current Internal Control Procedures Do Not Include Key IT Risk Management Practices

When reviewing the risk management procedures in the internal control policy, we identified Lottery's policy is out-of-date and no formal IT risk assessment is in place. Some specific examples of the issues we found are:

- The Lottery's policy identifies an internal audit function that no longer exists in the organization.
- The Lottery uses a spreadsheet tool titled "Risk Assessment" that is part of an annual internal control review, but this spreadsheet relates specifically to a change log policy and procedure and does not include a comprehensive identification of IT risk areas at Lottery.
- Industry standard IT security practices, including development of a security plan or security categorization for individual information systems, individuals, or assets are not conducted or documented.
- Some system vulnerability testing does occur, and Lottery staff do review the results, but there is no policy defining the process or how it should be coordinated with the overall risk assessment or internal control processes.
- Responsibilities are currently assigned to nontechnical staff without input from staff with the IT knowledge needed to identify and implement effective security practices.

While these gaps in policy and practice can be attributed to the internal control policy being out-of-date and referring to processes that do not exist within Lottery, the policy also does not fulfill the requirements of state policy or industry standards for IT risk assessments.

Lottery Should Adopt a Separate IT Risk Assessment Process

The Lottery has stressed the importance of annual review and participation in the risk assessment process and created the groundwork for an effective process through the internal control policy. However, this process is heavily focused on operational and accounting risks and has not yet incorporated proper IT risk assessment. At a minimum, the elements of an effective IT risk assessment should include:

- A risk assessment process for reviewing security control effectiveness along with the risk assessment environment, team, and each member's roles and responsibilities.
- An assessment of risks, including the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of information systems and the information they process, store, or transmit.
- Documentation of risk assessment results in a report that is reviewed annually by the Lottery director.
- Updates to the risk assessment process on an annual basis or when significant changes to the information systems or operations affect security, including new threats and vulnerabilities.

Because the Lottery does not currently have a defined IT risk assessment process, there are key IT security policies and procedures that have not been established. Specific examples of these issues are addressed in later sections of this report. In addition to addressing these more specific problems, the Lottery needs to develop an overall risk assessment framework for IT that formally guides its practices and decisions. Committing to a formalized risk assessment framework will help the Lottery better address threats to its IT infrastructure and effectively implement its organizational goals and objectives.

RECOMMENDATION #1

We recommend Lottery establish a risk management framework for information technology that aligns with state policy and industry standards.

Third-Party Assessment Results Were Not Completely Addressed

Lottery's operational activities involve large transactions, multiple vendors, and games of chance, increasing its overall risk. Therefore, Lottery is subject to evaluations from

various outside parties. These include Financial and Security audits conducted by the Legislative Audit Division (LAD) every two years, the Multi-State Lottery Association's (MUSL) periodic reviews of operations, and Federal Bureau of Investigation (FBI) audits of background check information.

Our audit work found the Lottery has not fully implemented recommendations made during these types of assessments. Recommendations made in the previous security audit report and the recent MUSL audit findings were reviewed. The implementation status of recommendations from our previous Lottery Security audit are discussed below.

- **Recommendation #1 – Partially Implemented**

  This recommendation relates to strengthening background check and ineligible player policy. Policy updates were made; however, they still were not clear enough to define contractors that needed background checks completed. Background checks for the internal control system contractor were initiated during fieldwork and background checks for the scratch ticket contractor are not completed.

- **Recommendation #2 – Partially Implemented**

  This recommendation speaks to strengthening investigative activity policy and documentation. A cover sheet and description of the investigation are required; however, these do not address the findings of the audit. The portion of policy and procedure that needs to be defined and improved is the supervisory review of investigations. This is where things like consistent documentation, appropriate investigation, and thoroughness can be addressed.

- **Recommendation #3 – Partially Implemented**

  This recommendation relates to establishing sales agent winners review procedures. A report was created to address this recommendation and was being used by the previous security director. However, the process was not clearly documented, and the current security director did not clearly understand the function of the report. Therefore, the report has not been created since the new security director took over in January 2017.

- **Recommendation #4 – Implemented**

  This recommendation addresses the review of sales agent record-keeping practices and sales. The assessment for retailers was reviewed and changes were made to the format and questions within the review. The purpose of the questions and why they are asked could be further clarified, but inventory procedures and record keeping for scratch tickets are addressed.

- **Recommendation #5 – Partially Implemented**

  This recommendation addresses the badge access system and establishing an access review procedure. While this recommendation was not implemented at time of review, Lottery did make efforts during fieldwork of this audit to improve the procedure. The recommendation is now partially implemented.

> Door labels within the system were updated during fieldwork. However, the review of the system was not documented thoroughly by the previous security director. Due to this, the review was not occurring in a manner that would identify inappropriate access or activity.

The recent audit conducted by MUSL also noted a repeat finding related to the Central Gaming System (CGS) contractor's security procedures. The finding addressed how the contractor manages and documents access to secure areas within their building containing ticket stock used in game terminals. While the Lottery is not directly responsible for the management of this procedure, the Lottery is responsible for ensuring contractor operations are secure and meeting MUSL reviews.

Lottery Risk Management Needs to Address Third-Party Assessments

Lottery's internal control policy addresses audit recommendations and indicates they are to be evaluated promptly and implemented on a timely basis. When discussing the implementation of past recommendations, Lottery staff clarified that the internal control policy was not intended to address external, third-party assessments and policy is only referring to internal audit reviews.

When discussing external reviews, or third-party assessments, like the security audit, Lottery staff indicated recommendations are a high priority and addressed as soon as possible, but they do not have a formal process for ensuring changes are implemented. Instead, the results are managed by the various directors within the Lottery. The intention is for the financial director to manage any financial audit recommendations, the security director to oversee the implementation of Lottery security audit recommendations, and the IT director to manage IT related audit recommendations. Regardless of who is responsible for the implementation, without a formal process for addressing third-party reviews, staff turnover will likely continue to impact recommendation implementation. Additionally, if recommendations or findings from audits go unaddressed, risks increase, impacting the integrity of Lottery operations.

In September 2016, the Lottery hired a new criminal investigator within the Security Division and in January 2017, a new security director was hired. As these are the only two security positions in the Lottery, a 100 percent turnover rate in a short amount of time impacted implementation of prior audit recommendations. While we agree that this contributed, it appears that partial implementation is an ongoing issue noted in previous Lottery Security audits. For example, a management memo was sent to the Lottery in the last audit cycle noting that the internal control procedures do not track audit recommendations effectively.

Including third-party assessment results in the risk management framework is an industry standard best practice and would reduce the impact of staff turnover. A well-rounded risk management process includes an established process for input from various managers, thoroughly vetting risks at an organizational level and a division level, and oversight and approval from the director. Including audit recommendations from external third parties in the risk management framework will provide an established process with the ultimate goal of ensuring the integrity and security of Lottery operations.

RECOMMENDATION #2

We recommend Lottery establish a process within the risk management framework that addresses the results of third-party assessments.

Chapter III – Information Security Policies & Staff Responsibilities

Introduction

Organizations implement effective information technology (IT) risk management processes as part of the overall IT security program. A strong program requires developing policies and procedures that align with business processes, while also enforcing and monitoring them to ensure they are effective. Defining who is responsible for these tasks and multiple other aspects of IT security, including risk management, is also crucial to a well-rounded security program.

While conducting fieldwork for objective 1, we identified that the Montana State Lottery's (Lottery) key security practices, like risk management, need further development. When reviewing who is responsible for these security practices, we identified Lottery has not assigned responsibilities in a way that ensures its IT security program aligns with state policy and industry standards.

This chapter will first discuss our review of job descriptions, information security responsibilities, and how the Lottery can better assign staff duties to ensure the program is effectively created, managed, and monitored. The latter sections will discuss the need for information security policies and training to ensure the IT security program is strengthened.

Defining IT Security Roles and Responsibilities of Lottery Staff Positions

Section 2-15-114, MCA, requires each department head ensure the security for all data within a department by:

- Designating an information security manager (ISM).
- Implementing appropriate, cost-effective safeguards to reduce, eliminate, or recover from identified threats to data.
- Ensuring internal evaluations of the security program for data are conducted.
- Including a general description of the existing security program and ensuring continued security of data is addressed in the agency information technology plan.

State policy provides further guidance on security roles for a well-rounded information security program. Roles discussed include senior management, security management, information security officers, program managers, system administrators, users, contract users, and other stakeholder groups. The policy also includes reporting

structures for effective and independent security management and the skills and abilities for successful information security management. The policy does note that not all positions discussed are available to every agency, but smaller agencies should combine responsibilities while still maintaining separation of duties and reducing any conflicts of interest. Common conflicts of interest for smaller agencies that need to be taken into consideration when assigning roles and responsibilities include:

IT Manager is also the ISM: While this may not be avoidable, it is not recommended because an IT manager would have the final decision as to what safeguards should be implemented and would be weighing these safeguards with efficiency. Safeguards are often minimized or disregarded to maintain or increase efficiency. Therefore, it is important to have multiple people involved in security management.

ISM reporting to IT Management: It is recommended the ISM report directly to the agency director or head instead of the IT director. This allows security staff to maintain independence and ensure security management is effective.

Reviewing/monitoring one's own activity: When assigning the responsibility of reviewing or monitoring any logs or activity reports, it is important to ensure a person is not reviewing their own activity. This person would be less likely to report issues with their own access or activity.

Overall, we identified that the Lottery's current staff assignments do not cover the requirements for information security. The following sections discuss how not having a dedicated ISM, or staff responsible to carry out key responsibilities, has caused multiple gaps between Lottery's information security practices and state policy requirements.

Lottery Staff Share Information Security Responsibilities, But More Coordination Is Required for Comprehensive Coverage

ISMs direct the day-to-day management of the information security program, including coordination of all internal and external security-related interactions. The ISM also maintains a documented security program for all agency staff to follow. The role of the ISM is critical in defending the integrity of the agency's IT infrastructure. The amount of policy and procedure that needs to be established and enforced can be substantial, and without a dedicated individual to perform this work, many aspects of security can be missed and leave an agency vulnerable from the inside or outside.

It is possible to have these responsibilities covered by multiple employees, but the roles need to be clearly defined in position descriptions. This is the approach the Lottery has taken to set up their information security program. Position descriptions for the

IT director, security director, and criminal investigator all include responsibilities within information security. However, the responsibilities described are high-level, and without more detail it is unclear how they meet the requirements of an ISM. The current responsibilities from job descriptions include:

IT Director:

- Research, develop, configure, and enforce network security policies and procedures.
- Ensure integrity and security during system testing.
- Develop, implement, and maintain the agency's local area network to ensure integrity and security.

Security Director:

- Duties include planning, developing, and administering a comprehensive security program for computer security.
- Knowledge of computer security requirements.

Criminal Investigator:

- Involved in all matters related to security, both computerized and physical.
- Twenty percent of job duties are specific to physical and computerized security.
- Knowledge of physical and computerized security protocol.

Information Security Responsibilities Are Misplaced and Unassigned

As part of our work, we compared these job descriptions with the responsibilities of the information security program to identify who should be overseeing key information security practices. Table 3 (see page 20) lists the IT security responsibilities of each organizational level based on state policy. The checks indicate where Lottery's current responsibilities from the job descriptions cover some of the requirements from state policy for a well-rounded security program.

Table 3

Comparison of Lottery's Position Descriptions to Information Security Responsibilities

	Information Security Policy: Roles and Responsibilities	IT Director	Security Director	Investigator
Security Management	Ensures information security policies & procedures are developed & maintained	✓	✓	✓
	Ensures management of common security controls			
	Ensures staff with significant responsibilities for system security plans are trained			
	Ensures adequate system security planning for department		✓	
	Ensures the organization-wide information security program is effectively implemented	✓	✓	✓
	Ensures information security considerations are integrated into all business or operational processes		✓	
	Ensures information systems are covered by an approved security plan & are authorized			
Information Security Officer	Evaluating real or suspected IT security incidents	✓		
	Providing resolution recommendations to agency head	✓		
	Developing policies, standards, & procedures in evaluating & referring investigations to law enforcement		✓	
	Carries out system security planning			
	Coordinates process of creating system security plans			
	Coordinates management of common security controls			
	Manages the common security controls			
	Reviews any changes to the system & assesses the security impact of those changes	✓		
Program Managers	Assists in developing the system security plan			✓
	Maintains the system security plan			
	Ensures the system is deployed & operated according to security requirements	✓		
	Ensures system users & support personnel receive requisite security training	✓		
	Updates system security plan when significant changes occur			
	Assists in management of common security controls			✓
	Establishes rules for appropriate use & protection of subject data/information			
	Decides who has access to information system & what types of privileges/access rights			✓

Source: Compiled by the Legislative Audit Division.

While there are general statements from each job description about IT security, the table shows that key duties are missing from all three. For example, it is unclear who is responsible for management of common security controls or ensuring staff with significant security responsibilities are trained. These responsibilities are not defined in Security or IT staff job descriptions or in Lottery policy and procedure. Consequently, employees do not clearly understand what is expected of them or how these duties support a complete information security program.

When reviewing how some of these key duties are carried out, we also identified duties that are misplaced in job descriptions and assigned duties that are not being fulfilled.

- While the criminal investigator (CI) is supposed to ensure the established security policies and procedures are followed, thorough IT policies do not exist for this to occur. The building access policy that does exist is managed by the CI who administers the badge access system, but IT and system access policies have not been established so this duty cannot be fulfilled.
- The investigator is also tasked with establishing access levels and privileges on network systems. This is assigned inappropriately for two reasons: the actual task of creating users and setting up access is carried out by IT staff or contractors and the task of establishing expected access levels and privileges on systems should be assigned to management-level positions responsible for programs or business functions. To ensure all aspects of security are accounted for, staff assigned security management responsibilities should also be involved in this process.
- The IT director is assigned the responsibility of establishing network security policies and procedures. While some procedures relative to the network exist, industry standard security practices are not included. Assigning this responsibility solely to the IT director is misplaced as it allows for a common conflict of interest by giving the IT director too much control over security measures. Industry standards assign this as a shared responsibility to ensure all aspects of security are considered and safeguards are not skipped to gain efficiency.
- The security director description overview assigns the position with responsibility for planning, developing, and administering a comprehensive security program for various aspects of Lottery, including computer security. However, further definition of what computer security means, or requires, is not included in the job duties, which leaves many specific responsibilities—like management of common security controls and system security planning—unassigned.
- The physical and computerized security job duties of the investigator state that the investigator is supposed to evaluate the security of multiple computer network systems and provide recommendations to maintain computer network system security. However, the job description requires no education or experience related to this field to effectively be able to carry out these duties. Only a mention of physical and computerized security protocols under

> "knowledge of" exists and no further policy or procedure within the security department assists to understand what level of knowledge is required for this position. Guidelines for this high-level responsibility indicate it is assigned to security management and senior management of an organization.

Due to these issues, it is unclear what security management practices are required for Lottery, who is responsible for them, and what level of knowledge they need to carry out these responsibilities. While the internal control policy lays out some detail that is related to the information security management responsibilities, it does not provide enough to clarify the issues identified within the job descriptions.

Lottery Needs to Clearly Define and Assign Information Security Manager Responsibilities

Without a well-defined security management program, the Lottery is at risk from multiple threats. While the most impactful would be a form of code manipulation or software and server tampering, there is also the potential for data to be stolen or misused. While there were not any incidents like this identified during the audit, there are examples from other Lotteries of what could happen when security responsibilities are not managed properly. Such as when the security director of Multi-State Lottery Association (MUSL) tampered with a random number generator to be able to predict winning numbers or when a former Texas Lottery employee copied the personal data of 89,000 players to a portable disc that was taken off-site after employment ended.

It is crucial the Lottery reevaluate and assign information security staff roles and responsibilities to ensure they are carried out effectively. This reevaluation will need to be completed with careful consideration for conflicts of interest due to its small organizational structure. For example, if the IT director were assigned all ISM responsibilities, Lottery would face conflicts with the IT director monitoring his or her own activity, putting them in the position of having to choose between efficient processes or security. Additionally, the responsibilities cannot all be assigned to the security director because this person would be monitoring his or her own activity and the current job description does not require knowledge in IT security to effectively carry out the duties. If the Lottery completes this evaluation and is unable to maintain separation of duties and address all conflicts of interest, it may need to consider developing a memo of understanding with the State Information Technology Services Division to conduct a portion of the security responsibilities or review other options for reassigning existing staff resources or requesting additional resources from the legislature.

RECOMMENDATION #3

We recommend Lottery:

A. *Evaluate and modify job descriptions for the IT Director, Security Director, and Criminal Investigator to clearly define IT security duties.*

B. *Integrate Information Security Manager responsibilities among these positions or seek additional means to address any issues with separation of duties or conflicts of interest.*

Lottery Has Not Developed IT Security Policy, Procedures, or Knowledge to Ensure Effective Security Controls

Within objective 1, we also wanted to determine if internal controls ensured the continuation of IT security in the case of turnover in key roles, such as the IT director or security director. Having documented security policies and procedures to pass on to new staff is an essential part of maintaining effective IT security.

While reviewing the Lottery's IT policies, security manuals, and position descriptions, we identified security policies and procedures for accounting, ticket stock management, physical access to the Lottery building, and general personal computer usage. However, documents specific to other aspects of IT security and Lottery operations were not present. These include documentation related to:

- Security Awareness and Training
- Security Plans and Architecture
- Personnel Security
- Access Management
- Risk Assessment

As an allocated entity, the Lottery relies on Department of Administration's resources and policies. However, the IT environment is unique within Lottery, and policies and procedures need to be in place that are relevant to Lottery. Additionally, security standards and state policy require well-defined policies and procedures as part of an effective security program. State IT security policies clearly state the need for safeguards to ensure that agency assets are not compromised, taken advantage of, or abused. When these policies are properly implemented, an agency is best equipped to deal with attacks on its systems and integrity.

Part of proper implementation of these procedures is ensuring all staff are knowledgeable of Lottery's unique security needs, as well as general IT security. Without this technical competence, safeguards will not be effective. For these reasons, statute requires the security director to have knowledge of computerized security. Additionally, the guidelines for security programs within state policy describe this knowledge as critical. The statute also requires a law enforcement background, which is important for investigations and managing retailer security. Current security staff have law enforcement backgrounds with some IT knowledge and experience; however, this experience is not specialized in IT security. If the Lottery continues to make the law enforcement background the focus of hiring security staff, it will also need to provide necessary training to prepare security staff for IT security management.

When reviewing job descriptions and roles and responsibilities of staff involved in IT security procedures, it will be important for Lottery to ensure a level of knowledge to effectively carry out assigned duties and continue education in IT security. By doing this, the Lottery can prevent IT security from falling behind new security requirements.

RECOMMENDATION #4

We recommend Lottery:

A. *Further develop and enforce required IT security policies and procedures that govern operations specific to the Lottery.*

B. *Ensure those tasked with information security management are knowledgeable and trained in information security management principles.*

Chapter IV – Computer and System Access Management

Introduction

Organizations are tasked with managing security at a time when information technology (IT) is becoming more mobile and portable and threats are becoming more sophisticated. Both technical, systematic controls and physical controls need to be established and reevaluated to ensure they are addressing changes and advancements in IT. Access management is one control concept used to ensure authorized access to an organization's data. Access management at the system level determines who can do what within a computer or system and monitors this activity, which is referred to as logical access. Access management also encompasses the physical access to hardware, like servers, which is discussed in Chapter V.

As part of our second objective, we reviewed governance over the technical controls of access management within Montana State Lottery (Lottery). System access management was reviewed from three angles:

1. **Governance:** Guidance established that creates policy and procedure to uphold access management principles that relate to Lottery.
2. **Standards:** Access management controls align with required standards and include those necessary for Lottery's situation.
3. **Control Review:** Current controls comply with policy and reduce risks to Lottery IT operations.

Overall, we identified that governance of physical access is taken seriously at the Lottery with dual authentication at most doors, cameras, and multiple documents outlining procedures and policy for managing building security. However, we also found management relating to securing computer, or logical, access is much more limited and is not governed in an equivalent manner. To ensure the integrity of Lottery operations, strong access management is required for its computer systems. While the threat of unauthorized access from outside sources is minimal, Lottery still has internal risks to address. Without strong access management, internal users could access gaming system code, security systems, and personal information; system functionality can be misused; or user access settings can be changed unknowingly. The following sections discuss our findings and the improvements that need to be made to access management by the Lottery.

Access Management Is Important Due to Lottery's Small Organization

The most common access controls are to enforce least privilege (allowing a user access only to tasks and information necessary for his or her normal duties) and segregation of duties (separating tasks within a procedure so one person cannot control the entire procedure and outcome.) The Lottery is a small agency, so there are multiple staff with multiple duties, especially in the Security and IT Divisions. To successfully implement least privilege and segregated duties, access must be managed upfront to prevent unauthorized access. There also needs to be equal emphasis put on monitoring access. Ongoing monitoring can detect and correct any incidents that occur due to excessive access from overlapping duties within the Lottery.

We identified that when the Lottery develops its formal IT security policies and procedures, it will need to address the following access management areas:

- Managing and reviewing user access.
- Enforcing the principles of least privilege and segregation of duties.
- Detecting unauthorized activity through system monitoring.

The following sections discuss our work in these areas with related findings and recommendations.

Formal Procedures for Managing and Reviewing User Access Are Needed

Industry standards and state policy require strong access management safeguards involved in granting, changing, and approving user access to prevent unauthorized user activity. Standards and state policy also require procedures for the ongoing review of this access to ensure it is kept current with user needs and detection of unauthorized access.

We reviewed access management policies and procedures related to multiple systems within the Lottery, including:

- The badge access system that manages the internal doors at the Lottery building,
- Back Office System (BOS) that is used for all administrative tasks to manage lottery games, drawings, retailers, and inventory,
- Internal Control System (ICS) that is used to verify BOS information, and
- The banking system used to pay prize money.

While Lottery has informal procedures for granting access to these systems, work needs to be done to formalize this process for all systems and create additional processes for required safeguards. We identified basic practices that need to be implemented, including:

- Formal documentation of the expected access for each role within a system had not been created. This information would be used to understand what access to set new users up with and what access users should have when reviewing access. Complete documentation of current user access was also not available. During fieldwork the Lottery was able to gather most of this documentation from contractors who manage operation and maintenance of the systems; however, some of the documentation did not show all users or all access assigned to that user.
- A complete process for granting, approving, changing, or terminating access has not been formalized. BOS has a consistent process of e-mail requests between the contractor and Lottery to establish, change, or remove accounts. However, other systems like ICS and the badge access system have no documentation or formal process for adding, changing, or removing accounts. E-mail communications for access management also did not include all requirements needed to establish access or formal authorization of access from the security director.
- Review of access or termination of access due to inactivity in most systems does not occur. The Lottery is a small organization and events requiring access changes, such as retirements or position changes, are well-known by all staff. A formal review would ensure that the changes are documented and occur in all systems. To complete this review effectively, the Lottery will need to develop accurate and detailed reports with contractors. We identified the user access reports gathered during fieldwork for BOS were not at a level of detail that would allow Lottery to review the exact access of users and the current user access reports for ICS did not include vendor access.

Access Security Is Underdeveloped for Multiple Lottery Systems

Because these basic practices to manage and review access have not been formalized, specific issues were identified within Lottery systems. Our work identified several issues within three main systems used by the Lottery. The following sections outline the issues identified within each system and the risks associated with each finding.

Badge Access System: When reviewing user access established in the badge security system for the internal doors of the building, we found a user's account was not removed at the time employment ended. A month later when the user list was requested, and the account was questioned, it was removed from the system. When employment ends, a checklist is used to ensure keys and badges are gathered from the person; however, it does not address deactivating or removing system accounts.

Test keys are used monthly to verify the system is working and guest keys for the badge security systems are provided for fire and police officers in case of emergency. These keys are not monitored and alerts for their use do not exist on the internal door system. The external alarm system does have a process to call the security director if the alarm is not deactivated when the door is opened. So, while there is a control for the exterior doors, the risk of misuse for these keys still exists if the key were to be used by someone with the external door code.

Back Office System (BOS): BOS manages all Lottery internal operations from accounting to scratch ticket inventory and winning number management. For the roles related to ticket inventory management, there is an access matrix showing the allowed access for each role within the system for the scratch inventory tracking system. However, it does not include all roles currently being used, like those by the contractor to manage ticket stock and system roles used to automatically change inventory status. Lottery staff required further details from the contractor to clearly identify these roles. User activity outside of inventory management is provided on a different report, but also had issues identified for the other functions within BOS. The report defined user access at a group of common functions, known as roles. Account management within the system also allows for individual differences to be made at the function level underneath the role. The report provided did not include some of these individual function differences for each user.

Further review of the user report identified two contractor employees who did not have background checks or personal files on record with the Lottery. These were verified as active employees, but they are not on the ineligible player list and do not have background checks. The ineligible player list documents who cannot play the Montana Lottery due to involvement in Montana operations. If the Lottery conducted a user review, these types of discrepancies would be identified.

Two accounts were identified in BOS for the security director, one for warehouse functions and one for security functions. According to Lottery staff, this is how the previous security director had access set up and due to the nature of access requests, this is how the new director was set up. Lottery access requests currently establish the same access as the predecessor in any position. While this makes requesting access easy and appear more efficient, it can lead to inaccurate access if the predecessor had any individual changes for specific situations or duties that do not apply to the new individual.

When reviewing recent access requests, an instance of access requested and authorized by the IT director with no documentation of the security director's approval was

identified. According to Lottery staff, the security director is the person who authorizes access to systems and has an informal e-mail process to do so, but in this instance, it was likely discussed between the directors and not documented.

A user activity report does not exist within the current reports available in the system. Policy and standards require user activity be logged or tracked and specifically notes the need for account management actions, like creation of users or change to access, to be logged. While Lottery staff stated the data should be available, it will have to be an effort in coordination with the contractor to get this report built. The contractor, who would provide the report, also has account management responsibilities in the system, so security of the report would need to be considered. The Lottery identified a feature the contractor uses with other clients that notifies the client any time an account is created, changed, or removed and has discussed implementing that in addition to the report that would provide activity to more than just account management activities.

Internal Control System (ICS): The Lottery has account managers established for this system internally and indicated the contractor has this ability as well. The user access screens reviewed during fieldwork did not show any contractor with access to the system. When discussing user access for the contractor, we identified unknown access levels are used by the contractor to manage the system. These access levels are of different authority than those granted to Lottery staff and due to system settings, are not available for Lottery staff to view. These roles have access to view user activity and manage accounts at different levels. The IT director has requested a higher level of access to obtain the ability to view user activity reports and contractor activity and access within the system. Activity within ICS is minimal in nature. The system has only a few fields for input and does not process information. Its main purpose is to verify the parameters for drawings done within the main Lottery system and ensure the main system has not been altered. While this reduces many risks related to the front-end application, Lottery staff still need the ability to see all access and activity within this system.

Because access changes are handled by Lottery staff for ICS, there is no formal authorization by the security director or process for account management procedures. Due to the inability to see contractor activity and access within the ICS application, neither the security director nor the IT director could see the contractor's actions, let alone authorize them.

Minimal Security Policies and Unclear Responsibilities Have Led to Incomplete Access Management

These specific issues occur when a security program is not well-defined through policy and procedure. This also occurs when responsibilities are unclear or improperly assigned to staff. While these are addressed previously in this report, it is still important for Lottery to establish user access management practices that include:

- Formal documentation so responsibilities are defined and easily transferred when staff turnover.
- Comprehensive procedures to ensure state policy requirements are met and risks to the Lottery are mitigated.
- User access reviews that occur periodically based on the level of risk or requirement by policy (monthly, annually, etc.) to verify access is appropriate.

Implementing these practices will help to prevent unauthorized access to data within all systems and ensure vital software is secure to safeguard the integrity of Lottery operations.

RECOMMENDATION #5

We recommend Lottery establish access control policies and procedures that encompass all systems including:

A. *Defined, documented procedure for granting, approving, changing, and removing access.*

B. *Periodic, documented user access reviews.*

C. *Complete documentation of current access of each user within each system.*

D. *Documented access level expectations for each user within the system.*

Key Access Management Principles

While the principles of least privilege and segregated duties are the most common access controls to ensure only authorized access occurs, they are only effective if clearly defined by access management policy and procedures. The Lottery has requirements within the internal control policy that center around accounting roles and duties that should be limited and segregated; however, roles related to IT security, such as account management and security, are not defined. The documented procedures related to segregation of duties and least privilege as well as industry standards for the general IT practices were used to review user lists for each system. Six user lists from

Lottery systems, varying from 10 to 50 employees each, were reviewed to ensure key access management principles were enforced. This review is discussed in the following sections.

Users Privileges Should Be Limited Throughout Lottery's Systems

The review of least privilege for each system identified instances of questionable access for certain users in Lottery systems. Audit work spent more time focusing on the roles and privileges within BOS, since the system manages all administrative tasks and ticket inventory, therefore posing the highest risk. Access in BOS and other systems, for the most part, is separated out and limited. However, there are key fields within BOS that should be further protected. These include:

- Four contractors have access to the ineligible player list managed by Security staff. This list dictates who is unable to play the Lottery due to being involved in operations. With access to this list and no activity monitoring, the contractor can go in and remove its own staff. This list also contains social security numbers of ineligible players. Therefore, access should be limited, as it contains confidential information.
- These same four contractors also have access to account management within BOS. Generally, this highly-privileged role is limited to one person and a backup so unauthorized changes to access for any user is less likely to occur and easier to monitor.
- A staff member within the Lottery's IT department had access consistent with operations level access used by the contractor that were not necessary for this position's current job duties. The analyst previously worked for the contractor and access was not adjusted when moving to work for Lottery.
- A sales representative within Lottery has general sales access within BOS as well as the accounting role access. When following up with Lottery staff, it was explained the accounting role was required for backup purposes. When reviewing the duties related to accounting access in the system, only specific account functions were needed, not all of them. The staff person previously worked in an accounting role and this access did not get evaluated when moving to the sales representative position.
- The contractor has staff that are required to have front-end access to BOS for their own job duties that support Lottery operations, such as ticket stock management. We identified multiple functions where the contractor "assists" as needed. Lottery staff explained that the contractor requires a broad range of access to the application to help troubleshoot issues and support Lottery activities. While contractor support may be needed, if it is not something done consistently as a normal, daily task, access "just in case" is not best practice and does not follow least privilege policy. Contractor staff, as users of the front-end system, should still be held to the same segregations and limited access as Lottery users. If these privileges are not removed and unauthorized access cannot be prevented, further work to monitor them will

have to be conducted by Lottery for detection of potential misuse. This is not currently occurring.

- When reviewing the badge access system, we identified a user with unnecessary access to the computer room, which contains the ICS server. Lottery staff stated this user was given access to the room during a remodel of the building because it is where a temporary workstation was located. After the workstation was relocated, access to the computer room was not removed.

Duties and Specific System Functionality Should Be Separated

Segregation of important access management tasks and general procedures within Lottery were reviewed for all Lottery systems as well. While some separations are noted in the Lottery's internal control document, the document is out-of-date and not followed by Lottery staff. The document also does not incorporate key IT separations, a definition of what should be reviewed, or risks that need to be reviewed when personal relationships occur. Because of not knowing what separations should exist and documenting them and any safeguards, there are segregations that are generally unacceptable within Lottery operations. These include:

- Random Number Generator (RNG) integrity includes a process to ensure certified versions of files are not tampered with. This process assigns a unique signature to each file in the form of letters and numbers. Whenever the RNGs are accessed, this signature is compared to the certified signature to make sure they match. This indicates no changes were made to the files that randomly select numbers. However, IT staff are the ones verifying the signatures, so they are monitoring their own activity, as well as the contractor, on the RNGs.
- Security staff who authorize access to systems, also have access and duties within most systems. This reduces the assurance that security access within the system is appropriate because staff in charge of access may be less likely to report issues or enforce least privilege.
- The contractor is currently responsible for creating users within the BOS system. Proper approvals need to come from Lottery staff before these accounts can be created for Lottery employees. Authorized contractor employees are approved through the background check process conducted by Lottery Security. However, the contractor can assign their own staff any level of access without further review by Lottery staff. The four contractor staff with access to account management also have access to various operational functions within the system which allows them to manage their own access.
- While discussing accountability and logging of activity of the ICS server, we found the reports that provide this information also log user names and passwords. Security staff have access to this information and access to log in to servers from the workstation because they have administrative profiles. While they do not have their own credentials to access a server, they can

easily use contractor usernames and passwords from these reports. Because Lottery security staff are also responsible for monitoring all ICS activity, they are in a position to use somebody else's credentials and evade detection.

Personal relationships among Lottery staff and contractors are considered a risk and procedures exist to document the relationship. However, further controls to ensure collusion does not occur within the authorized system access need to be considered and documented for effective review. Security staff are required to review specific relationships within the Lottery. We found that clear documentation of what risks the relationship poses or what security staff should be looking for when reviewing user access does not exist. Without the documentation of these unique risks, security staff cannot effectively review and monitor relationships to ensure the integrity of Lottery operations.

Lottery Needs to Document and Enforce Key Access Management Principles

Issues related to least privilege and separations of duties often occur in smaller organizations because the limited number of staff assuming dual roles. However, Lottery still needs to be aware of these principles and should not risk a security incident because someone is monitoring their own activity or authorizing their own access. Clearly defining the responsibilities of information security management will set the basis for these key principles, but further definition should be done to clearly document specifications relative to certain systems, procedures, and relationships.

RECOMMENDATION #6

We recommend Lottery improve access management by:

A. *Developing policies and procedures that enforce least privilege and segregated access for both internal and contractor staff.*

B. *Reviewing current contractor staff access and limiting privileged access.*

C. *Identifying and documenting privileged roles and any security requirements for those roles.*

D. *Clearly defining segregations for all systems, information security duties, and any additional controls required due to personal relationships within Lottery.*

E. *Including review of least privilege and segregation of duties when periodically reviewing access.*

Procedures to Detect Unauthorized Activity Need to Be Created

State IT policy requires organizations to identify users and verify their identities as a prerequisite to allowing access. The same policy also states that organizations need to create and maintain audit records to the extent needed to monitor, analyze, and report unlawful, unauthorized, or inappropriate activity. These two requirements are necessary to ensure the actions of unique users can be traced for accountability purposes. Without audit capabilities and enforcing accountability, it becomes very difficult to accurately detect issues that could compromise the integrity of Lottery operations in a timely manner. The following sections discuss our review of how the Lottery detects unauthorized activity in various systems and improvements that need to be made.

Lottery Needs to Ensure Identification and Authentication of Users Through Individual Accounts

At Lottery, identification and authentication practices, like password security practices and individual accounts, are being enforced for most systems. However, we did find several instances of shared user accounts being used, which are discussed as follows:

- The badge security system is on a workstation located in a security staff's office. At the time of our review, no access controls existed for the badge access system or the workstation, and no username or password was required to open the workstation or the badge access system. Additionally, access changes made by the security staff were not documented in an audit log or other documentation of access changes. This workstation also provides Lottery employees access to a system used in verifying winning tickets. While this process is assigned to security staff, warehouse staff also have access if backup is needed. This means that a warehouse employee could access this workstation and the badge security system to make any changes to door access or the door access system without being identified. While there is an activity report within the badge access system, it would not show what access was changed to and is not reviewed to identify these types of occurrences. As soon as Lottery was notified of these issues, individual accounts for both the system and workstation were created. Security staff explained that user names and passwords were not passed on from the previous staff and previous staff had also turned off the automatic screensaver at some point to stop having to log in to the workstation.
- Changes to the badge access system software would also go undocumented because there is no tracking or logging software on this workstation to identify workstation activity.
- Contractors access the ICS via a remote desktop connection approved by Lottery; however, the individual user is not verified as an approved user and a shared account is used by all contractor staff. This makes it hard for the Lottery to know if unauthorized contractor staff are accessing the ICS system.

- Within Lottery's building, there are two random number generators (RNGs) used for multiple games and for backup. These RNGs are under heightened security in a secured, secluded room. Physical access is controlled in this manner; however, logical access needs to be tightened. A shared account is used by security to authorize actions on the servers, server activity logs are not used or reviewed by Lottery staff, and general security measures such as password requirements are unknown. Due to the nature of these RNGs, specific physical and logical security precautions need to be established, and reviewed to ensure the security of these machines is maintained.
- Lottery staff use the same username and password to access a workstation within the computer room. This workstation is used to access BOS and personal e-mail only. While there is another layer of login information required on the workstation to access these applications, it is still good practice to use separate user profiles on the workstation.

Without enforcing individual accounts, accurate logging of user activity cannot occur and other means of verifying users, like surveillance video, would have to be used if it is available. While this is possible, it is not efficient and adds another layer of safeguards that are needed to ensure the videos are reliable and secure.

Monitoring Activity of Individual Users Needs to Be Established

Overall, there is minimal review of user activity reports to ensure users are held accountable for their actions. In most cases, the reports exist but are not reviewed and very few high-risk or unauthorized events are defined to understand the necessary security measures needed. The Lottery has some risks identified and, through other audits, has implemented safeguards. However, events within systems that can be considered high-risk to Lottery, such as changes to user access or changes to servers, have not been defined. Therefore, proper security measures, such as alerts and detective procedures, need to be established in various areas. Issues specific to individual systems and hardware that we identified include:

Back Office System (BOS): Activity reports do not currently exist in the system; however, the Lottery staff believe the data exists and they can work with the contractor to create the report. Not having activity reports impacts Lottery's ability to detect and hold internal and contractor users accountable for certain functions of higher-risk.

Badge Access System: The system does have activity reports defined by person and day; however, staff were unaware of any reports that would be defined by door. This makes monitoring access to specific doors, like those to rooms containing servers, more difficult and time-consuming. Another form of activity monitoring available to the Lottery is the video surveillance system. This system can be used in conjunction with the badge security system to monitor physical access. We found the system is slow

and does not have specific reporting or alerts. Currently, five to ten minutes of footage from each camera is reviewed each month to ensure the camera is still working and capturing the necessary activity, but the review is not effective for unauthorized access. With the speed of the videos and amount of footage it would be ineffective to have someone spend the time going through this video footage to identify improper access. Without a risk-based approach to this review, it would be unrealistic for staff to spend that amount of time reviewing the multiple cameras and 24-hour footage.

The system does not show specific activity related to account changes. It does note that changes were made but does not show what the changes were. Due to this, access management forms and documentation are needed to retain the details of these actions and should be used in coordination with the available reporting.

The badge access software is downloaded directly on the workstation used to access it. Accordingly, user activity tracking needs to be done for this workstation, like a server. This would ensure there is no unauthorized activity on the workstation that would interfere with the badge access system by making modifications to the software or workstation.

Internal Control System (ICS): Because the ICS servers are within the Lottery building, the contractor must request access through state fire walls and be granted access by Lottery whenever they need access. Contractor access to the ICS is requested through e-mail and logged on a hard copy file in the Lottery computer room. These files are compared to each other every six months to ensure access was granted to requested individuals. When comparing authorized individuals who have completed background checks from Lottery Security with the e-mails, we identified that one of the main users identified did not have a background check. Lottery IT staff authorize the requested access at the time of request, but do not verify the user was authorized by security staff.

Additionally, tracking software is installed on the workstation used to access the ICS application and servers. This software tracks keystrokes within the server and the application. While security staff were recently made to be the only staff with access to this software and information, it is not reviewed by security staff. By reviewing this report, the Lottery would be able to identify unauthorized activity instead of relying on random discovery through other means.

Random Number Generators (RNGs): Lottery uses a certified signature to verify no changes were made to the files on the RNGs used to randomly select numbers during Lottery drawings. While this is a valid way to ensure the files have not been tampered

with, audit logs to ensure unauthorized software has not been added in addition to these files are not reviewed. Whenever the RNGs are accessed, security and IT staff are present which would safeguard against this to an extent. However, security is not experienced enough in IT to know if unauthorized activities occur. The signatures are compared every time the RNGs are accessed, but this process is conducted by the IT director, without inclusion of the security director. For these reasons and due to state requirements, audit logging should be turned on and the security director should be included in these controls to ensure integrity.

Multiple Reasons Why Procedures to Ensure User Accountability Are Not Defined

One reason for issues like this is the choice for a more efficient way of operation over a more secure manner of operation. However, during fieldwork, Lottery staff were able to implement changes as the risks were identified, which shows increased emphasis and priority given to security controls. Other reasons contributing to these findings include the absence of reporting or system knowledge and undefined security program and responsibilities.

Information systems at the Lottery contain personal information, including social security numbers for ineligible players, and servers that hold applications and data relative to Lottery games are also on-site. It is important to properly identify and authorize users to ensure that activity being logged is unique to that user and that unauthorized activity can be prevented or detected. Without this, identifying exactly who should be accountable for any issues would be significantly harder and in most cases not timely.

RECOMMENDATION #7

We recommend that Lottery improve user activity tracking by:

A. *Ensuring individual user accounts and profiles are used on all workstations and systems and including requirements for individual user accounts when establishing access management policies and procedures.*

B. *Defining auditable events regarding all systems, databases, and physical locations.*

C. *Ensuring complete and accurate auditing or logging is available, secured, and reviewed relative to the risk associated with each auditable event.*

Chapter V – Physical Information Security Management

Introduction

Organizations are faced with more sophisticated security threats and increased vulnerabilities as information technology (IT) progresses and becomes more complex. To keep pace with these changes, managing how data is accessed requires evolving technical safeguards for users within systems, but these safeguards can become useless if unauthorized people can physically access hardware containing data. While the technical safeguards would be another layer to prevent data from being stolen or altered, destruction of hardware and data can be just as detrimental or costly. For this reason, access to rooms and areas where the Montana State Lottery's (Lottery) IT systems are located should be controlled in conjunction with system access.

The Lottery does have alarm systems and badge access systems to manage building and internal door security. However, this chapter discusses our review of IT access points and how these controls need to be improved to meet physical access requirements necessary to secure all IT access points.

General Security Practices Do Not Meet Information Security Requirements

The Lottery houses servers instead of having them at the state data center, so the requirement for physical security is heightened. This coupled with the requirement for the Internal Control System (ICS) to be completely separated from the Central Gaming System (CGS) provide unique security risks that the Lottery needs to consider. For example, the ICS backup and test environments are on servers physically located within the CGS contractor's building.

When reviewing security controls from policies, observations, and building tours, we identified the Lottery had numerous standard access controls and a few IT-related controls in place. However, standard access controls, like multi-factor authentication for doors and surveillance cameras, do not meet the information security requirements if implemented without effective review procedures. Additionally, if an overall assessment of an organization's inventory and corresponding risks have not been considered, all organizational weaknesses are not identified. By conducting this type of assessment, Lottery will be better able to identify and determine the most effective way to use standard access controls for IT security as well as identify areas where standard access controls do not mitigate IT risks and additional controls may be needed. Situations

where IT risks are not mitigated were identified throughout fieldwork and are discussed in this chapter.

Lottery Needs to Increase Physical Security Safeguards to High-Risk IT Areas

When reviewing physical security and access points of Lottery systems, we found basic controls including door access management, but we also identified areas where improvements are needed. For example, the badge system is limited in what is available for reporting to monitor physical activity and, during fieldwork, reports and functionality that security staff were not aware of were identified. This is because the system does not have a user manual and there was no knowledge transfer from previous security staff to current staff. The other areas identified include:

Badge Access System: The badge security system that manages physical security inside the Lottery building is located on a workstation within a security staff member's office. Security staff have keys to this room; however, other staff have access to this room and the workstation for high-value ticket validation. Procedures indicate they access this room in the absence of security staff as a backup. This room is not attached to any electronic alarm or security, so access to this room is not documented in the same manner as other doors. The doors are also locked by physical key and the Lottery does not include changing keys when staff turnover within security policies. Shortly after discussing the requirement for changing the locks on the door, Security staff indicated that all locks had been changed and door security for security offices is being increased.

Expectations for facility access in the Lottery's buildings or in contractor buildings are not clearly defined. Various access levels exist based on a role, just like an application, and best practices state the expectations should be defined by role to ensure access is granted properly. This documentation should also be considered when access is reviewed to ensure no unauthorized changes were made to the level of access that has been granted. Setting these expectations for contractors will also increase their compliance with state policy and other standards required of the Lottery by governing bodies like the Multi-State Lottery Association.

User access and activity are not reviewed through the badge system activity reports or surveillance footage to verify controls are working or to enforce best practices. This would reduce the amount of security issues like piggybacking or tailgating. This is when people try to enter facilities at the same time without being individually identified and authorized. When discussing these specific issues with Security, they stated they do not approve of it but know it occurs in certain doors. Audit staff had been let in by various Lottery staff without having to badge in to the front door throughout the audit.

Random Number Generators (RNGs): No list of authorized individuals with access to this room is kept or maintained by the Lottery. The procedure for authorizing access and accessing the room, including all security precautions is not up-to-date and does not include a verification of certified signatures or logical access precautions and controls.

The RNGs are not listed on the Lottery's IT inventory list. Previously this list was used for physical inventory managed by the Lottery and the RNGs were considered part of the contractor's system, not the Lottery's. While this is true, the RNGs physically reside within the Lottery building and need to be taken into account in inventory as part of risk management to ensure proper security controls are in place.

Internal Control System (ICS): Lottery staff not authorized to access the ICS server have access to the room where the server is located to conduct daily draw procedures. Various staff also come in this room for workstation setup. There is a camera pointed at the ICS server, but there is not an effective way of detecting misuse of computer room access. A person would have to sit through hours of video footage to ensure no one physically accessed the server because there are no access alerts at this time. These ICS servers are also not listed on Lottery's inventory list for the same reasons noted above.

Access privileges to this room are not reviewed regularly. There is also a discrepancy in how server rooms at the contractor location are required to be maintained and how this room, with a server, is maintained in the Lottery building. The contractor requires a log of anyone who accesses the room without credentials already given. This log is reviewed by Lottery staff as part of their six-month security checks at the contractor's building. The server room within Lottery does not have the same controls. When discussing this with Lottery staff, they stated the security procedure had never been established, most likely due to being a smaller organization where everyone is trusted.

ICS is independent of the Central Gaming System (CGS) because it is used to verify draw results and information within CGS. The backup servers for ICS are located within the CGS contractor's building. This poses a unique security situation for Lottery because the CGS contractor is not allowed to access the ICS server or system even though it is within their building. The room where the backup server is located has a badge and pin requirement as well as a key and lock. The contractor manages the badge and pin requirement as part of their building security system, so the key and lock managed by Lottery security staff ensures contractor staff are not giving themselves access to this room. When discussing how the Lottery would prevent the contractor from easily breaking the lock mechanism to get in the room and access servers, Lottery did not feel there was an immediate risk. They have a good working relationship with the contractor and trust them.

These situations and a trusting approach to IT security can leave organizations vulnerable to threats. Lottery began discussions with the ICS contractor for further controls during fieldwork. Through these discussions, Lottery identified additional controls exist, such as the option of real-time notifications being sent to security staff when the server is accessed. This would be a safeguard to detect if the key mechanism were compromised and unauthorized access to the ICS server were obtained. This along with a consistent process to review access logs and video footage should be established to better ensure the security of IT assets.

Physical Locations of Lottery's Servers Should Be More Secure

In May 2016, the governor signed an executive order calling for agencies to migrate their information technology assets to the enterprise infrastructure at the state data center. However, the Lottery prefers the gaming system servers be housed internally instead of at the state data center because additional security measures, such as background checks, are required for all individuals that have access to the servers. At the time of the audit, Lottery had not been granted an official exception from the executive order. Lottery indicated verbal approval was granted because the servers are proprietary to the contractors and should not be housed within the state data center. There are ways this can be coordinated with the state data center to meet Lottery's needs. Ultimately, it is the state chief information officer's (CIO) decision and exceptions for unique situations must be approved by the CIO.

Because these servers are on premises, higher security requirements are needed. The Lottery needs to protect and support the physical infrastructure of the information systems in addition to the logical security of firewalls and other measures provided by the contractors. Reviewing the best option for securing servers used by the Lottery and additional safeguards to secure other high-risk IT areas will decrease the risk of physical security breaches impacting the integrity of Lottery.

RECOMMENDATION #8

We recommend Lottery increase physical security by:

A. *Conducting and documenting analysis with the state chief information officer to determine the most secure location for servers.*

B. *Establishing and updating physical access policies and procedures regarding high-risk IT areas.*

C. *Establishing procedures for consistently monitoring physical access to alert or detect unauthorized access.*

MONTANA STATE LOTTERY

LOTTERY RESPONSE

MONTANA LOTTERY

September 17, 2018

Mr. Angus Maciver
Legislative Auditor
Office of the Legislative Auditor
State Capital Building
Helena, MT 59620-1705

RE: Response to the 2018 Montana Lottery Security Audit

Dear Mr. Maciver:

Thank you for the opportunity to respond to the report on the Montana Lottery Security Audit, dated September 7, 2018.

The Montana Lottery concurs with the audit findings and will take the necessary action to comply with all recommendations. In addition, security and information technology staff will conduct a review of the actions taken with Legislative Audit staff to ensure the issues are being properly addressed.

The following is our response and action plan to the specific recommendations of the audit:

RECOMMENTATION #1

We recommend Lottery establish a risk management framework for information technology that aligns with state policy and industry standards.

The Montana Lottery concurs with this recommendation and will incorporate an annual information technology (IT) risk assessment as part of the existing, over-arching internal controls review. This document is reviewed by the Information Security Administrators with the Director. The assessment will focus on protecting the Lottery IT infrastructure from any action having a negative impact on Lottery operations and will be documented in Lottery policy and procedures.

The development of this assessment will be completed utilizing input from existing industry standards and policy from the State Information Technology Services Division (SITSD).

RECOMMENTATION #2

We recommend Lottery establish a process within the risk management framework that addresses the results of third-party assessments.

The Montana Lottery concurs with this recommendation and will include a review process of third party assessments within the current internal control process. In addition, Lottery will work to establish a review of the planned actions with the assessment authors. This review will help ensure Lottery is properly addressing the recommendation and to safeguard against issues that can arise from staff turnover.

RECOMMENTATION #3

We recommend Lottery:

A. **Evaluate and modify job descriptions for the IT Director, Security Director, and Criminal Investigator to clearly define IT security duties.**
B. **Integrate Information Security Manager responsibilities among these positions or seek additional means to address any issues with separation of duties or conflicts of interest.**

The Montana Lottery concurs with this recommendation and will modify the current job descriptions to clarify duties and address the role of the Information Security Manger and the responsibilities outlined in existing SITSD policy. These changes will also be reflected in Lottery policy and procedures and supported with compensating controls when conflicts arise.

With the ever-increasing role that information technology plays in daily operations, the need for a dedicated Information Security Manger becomes apparent. Lottery will explore all possibilities to fill this key piece of the security puzzle to include contracting and a dedicated position.

RECOMMENTATION #4

We recommend Lottery:

A. **Further develop and enforce required IT security policies and procedures that govern operations specific to the Lottery.**
B. **Ensure those tasked with information security management are knowledgeable and trained in information security management principles.**

The Montana Lottery concurs with this recommendation and will continue to develop and improve security policies and procedures. Several areas have been identified to include access management, IT architecture and personnel security. In addition to the procedures proper documentation of all actions taken will be included.

Lottery will identify specific training needs for the individuals assigned to IT security roles. This will include developing a detailed training plan, so staff can successfully understand, implement and refine IT security policies and procedures.

RECOMMENTATION #5

We recommend Lottery establish access control policies and procedures that encompass all systems including:

A. **Defined, documented procedure for granting, approving, changing, and removing access.**
B. **Periodic, documented user access reviews.**
C. **Complete documentation of current access of each user within each system.**
D. **Documented access level expectations for each user within the system.**

The Montana Lottery concurs with this recommendation and will formalize, improve and document methodology for access to Lottery systems. A review of current access and duties of all positions, including contractors, will be used to define the level of access needed and to help create Access Management Policy and Procedures. All access will be documented and a periodic review of access and supporting documentation will be conducted to help ensure the integrity of the system. Lottery has already started to address this recommendation through developing an accurate inventory of positions with descriptions and defining the roles and level access within our systems.

RECOMMENTATION #6

We recommend Lottery improve access management by:

A. **Developing policies and procedures that enforce least privileged and segregated access for both internal and contractor staff.**
B. **Reviewing current contractor staff access and limiting privileged access.**
C. **Identifying and documenting privileged roles and any security requirements for those roles.**
D. **Clearly defining segregations for all systems, information security duties, and any additional controls required due to personal relationships within Lottery.**
E. **Including review of least privilege and segregation of duties when periodically reviewing access.**

The Montana Lottery concurs with this recommendation and will develop an access management policy and procedure that addresses the definition of privileged access, defining when that access is appropriate, limiting privileged access, and determining when shall it be suspended. Monitoring will be accomplished by the assigned IT security administrator and occur on a regular basis.

A review of Lottery systems has already been completed with individual contractors and staff privileged access being identified. These individuals fell into two categories, the first being elevated access because of additional duties; and second, the individual had inherited access because they replaced an individual with additional duties. Those with elevated access without a business need have had their access scaled back.

RECOMMENTATION #7

We recommend that Lottery improve user activity tracking by:

A. **Ensuring individual user accounts and profiles are used on all workstation and systems and including requirements for individual user accounts when establishing access management policies and procedures.**
B. **Defining auditable events regarding all systems, databases, and physical locations.**
C. **Ensuring complete and accurate auditing or logging is available, secured, and reviewed relative to the risk associated with each auditable event.**

The Montana Lottery concurs with this recommendation and will ensure both physical and virtual access to the Lottery and Lottery systems are tied to a single user by using a robust access management policy, physical control and auditing.

RECOMMENTATION #8

We recommend that Lottery increase physical security by:

A. **Conducting and documenting analysis with the state chief information officer to determine the most secure location for servers.**
B. **Establishing and updating physical access policies and procedures regarding high-risk IT areas.**
C. **Establishing procedures for consistently monitoring physical access to alert or detect unauthorized access.**

The Montana Lottery concurs with this recommendation and has moved appropriate servers to the state data farm. Lottery has consulted with SITSD and obtained a written exemption for moving the remaining servers based on security and the needs of the Lottery. Physical security for the location of the remaining servers will be updated to provide better monitoring capabilities. Policies regarding access to high-risk IT areas will be updated to reflect all changes.

Thank you again for the opportunity to respond. Your team established a good rapport with our office and showed strong professional knowledge and personal professionalism while working with the Lottery.

Sincerely,

Angela Wong, Director
Montana Lottery

Audit Recommendation	Lottery Response	Corrective Action Plan	Responsible Area	Target Date
RECOMMENTATION #1 **We recommend Lottery establish a risk management framework for information technology that aligns with state policy and industry standards.**	Concur	• Restructure and update the Internal Control Policy to include a separate section specifically called Information Technology Security Policy. • Rename current "Risk Assessment" spreadsheet to "Operational Risk Assessment and Desk Manual Change Log" and create a separate new "Information Technology Security Risk Assessment." This document will define the assessment of risk associated with IT systems/assets based on function. IT system administration and user interaction with these systems/assets will also be documented with associated risks defined based on exposure and potential threat. • The IT Security Policy will also cross-reference requirements provided in the SITSD POL-Information Security Policy directly with Lottery specific IT assets and resources. • IT Security Procedures referenced in the new IT Security Policy will be created or updated to ensure existing risks are being monitored, new risks are identified and mitigated, and documentation is current. • Staff responsible for the management of the IT Security Policy will be trained internally through the details provided within each policy and procedure, and externally via Information Security training online courses, classes, or available seminars to ensure they are managing the policy and process as effectively and efficiently as possible. • IT security administrators will also periodically review policy and procedure with the Lottery Director to ensure documentation is current and security controls are in place to manage defined risks. *Policies, procedure and forms impacted (current and new)* *Information Technology Security Policy* *Information Technology Security Risk Assessment*	MT Lottery IT (primary) MT Lottery Security	Mar – 19 Mar – 19

		IT Security Procedures for (each IT asset/resource) *IT Security Verification Form/Log for (each IT asset/resource)* *IT Security Administration Review Procedures* *IT Security Administration Review (sign-off form)*		
RECOMMENTATION #2 **We recommend Lottery establish a process within the risk management framework that addresses the results of third-party assessments.**	Concur	• The action plan for recommendation 1 includes the creation of a separate "Information Technology Security Risk Assessment." This document will also be used to maintain a list of all prior Legislative Audit, Multi-State Lottery Association (MUSL), or all other audit/review findings and corresponding responses. These findings and responses will include specific finding details and Lottery determined action plans to mitigate the associated risks. • A procedure will be created to ensure all IT security administrators periodically review and confirms risks associated with each item are still being mitigated. • Recommendations made during the previous security audit will also be included in the Information Technology Security Risk Assessment to be tracked. Partially implemented recommendations will be fully implemented and reviewed with the Legislative Audit staff to ensure the issues have been properly addressed. *Policies, procedure and forms impacted (current and new)* *Sub-section of Information Technology Security Risk Assessment, labeled Prior Audit Findings* *IT Security Administration - Prior Audit Findings Review Procedures* *IT Security Administration - Prior Audit Findings Review (sign-off form)*	MT Lottery IT (primary) MT Lottery Security	Mar – 19 Mar – 19
RECOMMENTATION #3 **We recommend Lottery:** **A. Evaluate and modify job descriptions for the IT Director,**	Concur	3A • Establish the role each IT security administrator is responsible for based on the updated policy and procedures. • Update each job description to ensure specific responsibilities are defined under a new subsection "IT Security Duties"	MT Lottery IT (primary) MT Lottery Security	Jun – 19 Jun – 19

Security Director, and Criminal Investigator to clearly define IT security duties. **B. Integrate Information Security Manager responsibilities among these positions or seek additional means to address any issues with separation of duty or conflicts of interest.**		• Define each responsibility in a supplement to the job description; why the position is responsible for this duty and how they will accomplish it. • The Lottery Director will also ensure there are no conflicts of interest present for each responsibility, nor any single position is tasked with monitoring their own personal functions. Compensating controls must be clearly defined and periodically reviewed. *Policies, procedure and forms impacted (current and new)* *IT Security Duties (supplement to each job description)* *IT Security Duty Annual Checklist (sign-off form)* 3B • All bullet points in table 3 (page 20) of Information Systems Audit will be assigned to a responsible party. An IT Security Duties Policy will be created with all Information Security responsibilities clearly defined and the corresponding responsible party. Risks will be included along with compensating controls. The Lottery Director will also review this policy with the IT security administrators as part of the annual checklist review. • If a responsibility cannot be effectively managed internally through compensating controls, the Lottery will investigate possibilities to fill this key piece of the security puzzle to include contracting a dedicated position. *Policies, procedure and forms impacted (current and new)* *IT Security Duty Policy (chart with descriptions and positions covering)*		Jun – 19
RECOMMENTATION #4 **We recommend Lottery:**	Concur	4A In correlation with the action plan defined for recommendation 1, the following policies and procedures will also be included:	MT Lottery IT (primary)	Mar – 19

A. Further develop and enforce required IT security policies and procedures that govern operations specific to the Lottery. **B. Ensure those tasked with information security management are knowledgeable and trained in information security management principles.**		• Security Awareness will incorporate new hire and annual review of cyber security requirements, Lottery workstation/laptop/IT asset security training and privileged user security documentation. End user documentation will be created/updated with an all-inclusive verification of completion. IT security administrator verification procedures will also be created. • IT Security Plans and Architecture will define Lottery-centric IT infrastructure including all IT assets and their function, admin and users of these assets, and risks and security requirements defined for each asset. • Personnel Security and Access Management will include many layers, such as policy, forms and procedures for IT security administrators that will define each Lottery position, access privileges required for the position, risks associated with the access granted, risks if additional access is granted, and potential risks associated with relationships to other positions. The form will be used to ensure proper access is granted on hire, or when changes are made to the position or user responsibilities are altered, as well as when users leave their current position. IT security administrator will review these forms while performing periodic review of access. As noted with the action plan defined for recommendation 1, the Information Technology Security Risk Assessment will include risks associated with each specific Lottery system/asset and user. *Policies, procedure and forms impacted (current and new)* *Security Awareness Policy* *Security Awareness Review Procedure* *IT Security Plans and Architecture documentation* *Access Management Policy* *Access Management Form*	MT Lottery Security	Mar – 19

		Access Management Procedure 4B As noted in the response to recommendation 1, all IT security administrators will be trained internally through the details provided in the various policies they are responsible for. Additionally, external training via Information Security online courses, or available seminars will be considered to ensure the IT administrators are managing those policies and processes as effectively and efficiently as possible.		Mar - 19
RECOMMENTATION #5 **We recommend Lottery establish access control policies and procedures that encompass all systems including:** **A. Defined, documented procedure for granting, approving, changing, and removing access.** **B. Periodic, documented user access reviews.** **C. Complete documentation of current access of each user within each system.** **D. Documented access level expectations for each user within the system.**	Concur	5A As noted in response to recommendation 4, an Access Management Policy, Access Management Form, and Access Management Procedure will be formalized to document access privileges by position. The Access Management Form will define user privileges via position. All system access will be defined in one form, with add/change/delete fields and the necessary approval permission fields. These forms will also be maintained for historical record. 5B Access Management Procedures will define how the Access Management Forms are maintained and reviewed to ensure any changes have been made correctly, and that no undocumented changes have taken place. Periodic reviews will be required, and verification of these periodic reviews will be confirmed by the Lottery Director. 5C Access Management Procedures will include current documentation of all access within each system. Periodic user reviews will also include the review of each system to ensure no undocumented changes have occurred. Care must be taken to ensure no IT security administrator is reviewing their own access. Compensating controls must be in place for these reviews. Compensating controls will be defined in the Access Management Procedure. The periodic user access review will take	MT Lottery IT (primary) MT Lottery Security	Mar – 19 Mar – 19 Mar – 19 Mar – 19

		place monthly. The annual review of compensation controls, as well as verification that the user access reviews are occurring will be conducted annually with the Lottery Director and IT security administrators. 5D Access Management Procedures will outline specific position level access for all systems, risks associated with the granted access, and any potential threats with additional access granted (what each position should, and should not have access to, and the risks associated with that additional access).		Mar – 19
RECOMMENTATION #6 **We recommend Lottery improve access management by:** **A. Developing policies and procedures that enforce least privileged and segregated access for both internal and contractor staff.** **B. Reviewing current contractor staff access and limiting privileged access.** **C. Identifying and documenting privileged roles and any security requirements for those roles.** **D. Clearly defining segregations for all**	Concur	6A As noted in the response to recommendation 4 and recommendation 5, Access Management policies and procedures for each IT system will define risks associated with each access level and will include clear details to enforce least privilege, segregation of access and duties, and how to manage this requirement. Access Privileges will be defined by position level and will also include supporting contractor staff. 6B Access Management Procedures will include detailed instructions of periodic access level reviews, including current access settings with details on why the settings are defined as such, what to watch for, what access privileges to prevent and why for both Lottery and contractor staff. 6C Access Management Procedures will clearly define security requirements and limitations set for all roles including elevated roles. This detail will be used to ensure least privileged are only granted privileged access as needed, with risks assessed, documented and monitored. 6D	MT Lottery IT (primary) MT Lottery Security	Mar – 19 Mar – 19 Mar – 19 Mar – 19 Mar – 19

systems, information security duties, and any additional controls required due to personal relationships within Lottery. **E. Including review of least privilege and segregation of duties when periodically reviewing access.**		Access Management Procedures will define the segregation of the management of Information Security duties to ensure IT security administrators are not monitoring their own activity. Compensating controls will also be clearly defined with associated risks addressed. Personal relationships within the Lottery will continue to be documented on a case by case basis. This documentation will be updated with additional detail to specifically address Information Security risks and define any necessary compensating controls to reduce that risk. IT security administrators will periodically review this segregation of Information Security duties and personal relationship data with the Lottery Director. *Policies, procedure and forms impacted (current and new)* *Personal Relationship Policy Supplement (specifically addressing Information Security Risks)* 6E Access Management Procedures will include the review of least privilege and segregation of duties by the IT security administrators semi-annually, with a follow-up review with the Lottery Director annually.		Mar – 19
RECOMMENTATION #7 **We recommend that Lottery improve user activity tracking by:** **A. Ensuring individual user accounts and profiles are used on all workstation and systems and including requirements for individual user**	Concur	7A A separate standalone workstation will be provided to the Security Department to move all secondary software off the workstation hosting the Badge Access System. This workstation will be documented and managed like the Badge Access System workstation, but with its own separate risks and management defined. When the Random Number Generator (RNG) server room needs to be accessed, separate user accounts will be defined on each RNG server for the IT Director and Criminal Investigator. Additionally, enabling audit logging is being currently investigated by the contractor. This	MT Lottery IT (primary) MT Lottery Security	Mar – 19 Mar – 19

accounts when establishing access management policies and procedures. **B. Defining auditable events regarding all systems, databases, and physical locations.** **C. Ensuring complete and accurate auditing or logging is available, secured, and reviewed relative to the risk associated with each auditable event.**		will also be enabled after the contractor and Lottery confirm the relative data being audited. As noted in the response to recommendation 6, access management policies and procedures will clearly define individual position user access requirement for each IT system. *Policies, procedure and forms impacted (current and new)* *Access Management Procedure (addition to ensure user activity tracking per system)* 7B Policies and procedures used by all IT security administrators will be documented to clearly describe the requirements to perform those administrative responsibilities; acceptable events, unexpected events and additional steps that need to be taken. *Policies, procedure and forms impacted (current and new)* *Access Management Procedure (addition to ensure event triggers are acted upon)* 7C Auditing will be enabled on defined systems and procedures used to review activity will be clearly defined with all the necessary details and actions required. *Policies, procedure and forms impacted (current and new)* *Access Management Procedure (addition to include detailed auditing instructions)*		Mar – 19 Mar – 19
RECOMMENTATION #8	Concur	8A	MT Lottery IT	Sept – 18

We recommend that Lottery increase physical security by: **A. Conducting and documenting analysis with the state chief information officer to determine the most secure location for servers.** **B. Establishing and updating physical access policies and procedures regarding high-risk IT areas.** **C. Establishing procedures for consistently monitoring physical access to alert or detect unauthorized access.**		In 2017 the Lottery and SITSD successfully moved the Lottery office fileserver onto the enterprise infrastructure at the state data center. The contractor supplied Lottery Operating System servers are primarily housed and maintained at the contractor facilities per contract. However, the (Internal Control System) ICS and RNG servers are housed and maintained at the Lottery facility which is allowed by an exemption from the State Chief Information Officer after review and consideration by the Lottery and the state CIO. This formal exemption will be reviewed annually by the Lottery and state CIO to ensure terms and conditions are maintained. 8B The Lottery will be updating or generating Physical Access policies and procedures to ensure assets are secured, physical access is reviewed, tracking is defined clearly, and reviewing accountability is achieved. *Policies, procedure and forms impacted (current and new)* *Information Systems Physical Security Policy* *Information Systems Physical Security Procedures for (each IT asset/resource)* *Information Systems Physical Security Form/Log for (each IT asset/resource)* *Information Systems Physical Security Review Procedures* *Information Systems Physical Security Review (sign-off form)* 8C The Lottery will determine a solution to track physical access into all high-risk security areas that will allow the Security department the ability to consistently detect unauthorized physical entry. Procedures and logging will be created to ensure monitoring and the periodic review of physical entry. This review will allow the Security department to take necessary action if an unexpected activity is	MT Lottery Security (primary)	Sept – 18 Mar – 19 Jun - 19

		discovered. These measures and procedures will be enabled to regularly detect unauthorized access and ensure accountability.		